Lecture 17

In this lecture we continue our study of algorithms, focussing on an extension to the Euclidean algorithm and on primality testing.

Extension to the Euclidean algorithm

If $d = \gcd(m, n)$

then d can be expressed as a linear combination

$$\boxed{d = xm + yn}$$

of m and n, where x and y are integers.

To find x and y, we work back through the steps of the Euclidean algorithm from bottom to top.

For example, it can be shown that $\gcd(22, 96) = 2$:

$$96 = 4 \cdot 22 + 8$$

$$22 = 2 \cdot 8 + 6$$

$$8 = 1 \cdot 6 + 2$$

$$6 = 3 \cdot 2$$

Now we use the second-last line to make 2 the subject of the equation:

$$2 = 8 - 1 \cdot 6$$

Next we use the third-last line to express 6 in terms of 22 and 8, substituting this into the equation we've just produced:

$$\begin{aligned} 2 &= 8 - 1 \cdot 6 \\ &= 8 - 1 \cdot (22 - 2 \cdot 8) \\ &= 8 - 1 \cdot 22 + 1 \cdot 2 \cdot 8 \\ &= 3 \cdot 8 - 1 \cdot 22 \end{aligned}$$

Finally we use the fourth-last line to express 8 in terms of 96 and 22, substituting this into our most recent equation:

$$\begin{aligned} 2 &= 3 \cdot 8 - 1 \cdot 22 \\ &= 3 \cdot (96 - 4 \cdot 22) - 1 \cdot 22 \\ &= 3 \cdot 96 - 3 \cdot 4 \cdot 22 - 1 \cdot 22 \\ &= 3 \cdot 96 - 13 \cdot 22 \end{aligned}$$

Here's another example. It can be shown that the gcd of 63 and 256 equals 1:

$$\begin{aligned} 256 &= 4 \cdot 63 + 4 \\ 63 &= 15 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

Then we work upwards from the second-last line, as follows:

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (63 - 15 \cdot 4) \\ &= 4 - 1 \cdot 63 + 1 \cdot 15 \cdot 4 \\ &= 16 \cdot 4 - 1 \cdot 63 \\ &= 16 \cdot (256 - 4 \cdot 63) - 1 \cdot 63 \\ &= 16 \cdot 256 - 64 \cdot 63 - 1 \cdot 63 \\ &= 16 \cdot 256 - 65 \cdot 63 \end{aligned}$$

So we have successfully expressed 1 as a linear combination of 256 and 63.

In this example, 63 and 256 are <u>relatively prime</u> (which just means that their gcd equals 1).

Technically, what we have done is essentially to find the "multiplicative inverse modulo 256" of the integer 63. This technique is essential for finding the secret key in the **frequently used** RSA-cryptosystem. (We omit any further details of this.)

Prime numbers play a vital role in coding and cryptography. A prime number is an integer > 1 which has no factors other than itself and 1. So the first ten prime numbers are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

But suppose that we want to produce the first 100 prime numbers, as a list. We need an algorithm to do this.

One such algorithm is described in the textbook on pp. 76—78. We modify it slightly.

Firstly we write down 2 as the first prime number. After that, we start testing the odd numbers from 3 onwards. The key idea is that we try to divide the odd number by all the odd numbers which are less than or equal to that odd number (and are greater than 1).

If we find a divisor less than the given odd number, we stop and declare that the given number is not prime.

We use the following variables:

K = desired no. of primes

k = the counting index no.

$p_1, p_2, \ldots, p_K$ are the primes being sought

i = the no. being tested for primality

j = a possible divisor of i

ℓ = the smallest (>1) divisor of i

Note that i is prime if and only if $i = \ell$.

We use the notation

$$j \mid i$$

to mean "j divides i" (that is, j is a divisor of i).

So:

- K is fixed;
- k ranges from 1 to K, and increments after a prime is found;
- i starts at 2, then goes to 3, and then increments by 2 after the primality testing of the current value is complete;
- j ranges from 3 to i, incrementing by 2 after the current value is tested as a possible divisor of i (but j stops incrementing as soon as it reaches a value which divides i);
- l equals the largest value of j (which is also the smallest divisor of i);
- p_k = the current value of i if $i = l$ (so that i is prime), and if $i \neq l$ then we keep searching for the next prime number.

The following table shows how the algorithm produces the first five prime numbers.

count	possible prime	possible divisor of i	True or false?	smallest divisor (>1) of i	True or false?	k^{th} prime
k	i	j	$j \mid i$	ℓ	$i = \ell$	p_k
1	2	–	–	–	–	2
2	3	3	T	3	T	3
3	5	3	F			
		5	T	5	T	5
4	7	3	F			
		5	F			
		7	T	7	T	7
5	9	3	T	3	F	
	11	3	F			
		5	F			
		7	F			
		9	F			
		11	T	11	T	11

The last column tells us that:

$$p_1 = 2$$

$$p_2 = 3$$

$$p_3 = 5$$

$$p_4 = 7$$

$$p_5 = 11$$

In other words, the first five primes are 2, 3, 5, 7 and 11.